



①9



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

①1 Número de publicación: **2 332 033**

⑤1 Int. Cl.:
G06T 1/00 (2006.01)

①2

TRADUCCIÓN DE PATENTE EUROPEA

T3

⑨6 Número de solicitud europea: **00945910 .8**

⑨6 Fecha de presentación : **12.07.2000**

⑨7 Número de publicación de la solicitud: **1303837**

⑨7 Fecha de publicación de la solicitud: **23.04.2003**

⑤4 Título: **Imágenes digitales filigranadas.**

④5 Fecha de publicación de la mención BOPI:
25.01.2010

④5 Fecha de la publicación del folleto de la patente:
25.01.2010

⑦3 Titular/es: **Motorola Limited**
Jays Close, Viabes Industrial Estate
Basingstoke, Hampshire RG22 4PD, GB

⑦2 Inventor/es: **Hobson, Paola, Marcella y**
Tay, Lai, Hock

⑦4 Agente: **Ungría López, Javier**

ES 2 332 033 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Imágenes digitales filigranadas.

5 **Campo de la invención**

Esta invención se refiere a imágenes digitales filigranadas. En particular, se refiere a métodos para mejorar la confianza en imágenes digitales filigranadas y para su autenticación.

10 Con el fin de aumentar la confianza del uso de imágenes digitales como prueba, posiblemente en un tribunal de justicia, hay una importante necesidad de demostrar que una imagen no ha sido manipulada.

Antecedentes de la invención

15 Es conocido usar análisis de auditoría, en que se adjunta a la imagen información acerca de cuándo se procesó una imagen, pero estos métodos son solamente aplicables una vez que una imagen ha sido registrada en un sistema. Por lo tanto, dicho análisis de auditoría no puede detectar operaciones no autorizadas antes del registro en un ordenador, y puede no ser capaz de informar acerca del tipo de procesamiento realizado en cualquier momento. El análisis de auditoría también puede ser evitado o corrompido, ya sea deliberadamente o de forma accidental.

20 La filigrana de la imagen es una técnica conocida. En esta técnica, se incrusta una configuración binaria conocida o firma en una imagen en el momento de la adquisición de la imagen. Tales filigranas se denominan “robustas” porque están diseñadas para permanecer intactas independientemente de cualquier procesamiento posterior de la imagen tal como filtración, recorte, etc. Aunque tales filigranas proporcionan un grado de protección útil, actualmente no se puede
25 confiar plenamente en ellas no pueden tener siempre el grado necesario de seguridad de que una imagen no haya sido manipulada para usar la imagen como prueba bajo las normas estrictas de los tribunales de justicia, etc.

Ruanaidh, Dowling y Boland “Phase Watermarking of Digital Images”, IEEE INTCONF Image Processing, Vol. 3, Lausanne, Suiza, septiembre 1996, p. 239 a 242, describe una técnica para filigranar imágenes digitales en que una
30 imagen se divide en bloques de un tamaño seleccionado (por ejemplo 16 x 16 píxeles). Se aplica una transformada Fourier discreta (DFT) al componente de luminancia de la imagen en base de bloque a bloque. La DFT es un valor complejo y por ello genera un módulo y una fase. La filigrana resultante incluye una cadena binaria de 1s y 0s que puede representar, por ejemplo, un logo de compañía, un código de autenticación de usuario, información de fecha/hora/posición, etc. La filigrana se incrusta en la imagen alterando la fase de los coeficientes DFT seleccionados.

35 Un artículo titulado “Attack Characterization for Effective Watermarking” por Deepa Kundur y Dimitrios Hatzinakos, Conferencia Internacional sobre Procesado de Imágenes, ICI P’99, Kobe, Japón 24-28 Octubre 1999, páginas 240-244, describe un esquema de filigrana en el que se incrustan dos filigranas (una filigrana robusta y una filigrana de referencia) en una imagen con el fin de llevar a cabo la recuperación de la filigrana robusta en caso de ataque a la
40 imagen. La filigrana de referencia (es conocida por el dispositivo receptor) y se usa para caracterizar un ataque antes de que la filigrana robusta sea recuperada permitiendo por ello que la filigrana robusta sea decodificada más exactamente.

La presente invención surgió en un intento de proporcionar un método mejorado de autenticar una imagen filigranada y de mejorar por ello la confianza en ella.

45 **Breve resumen de la invención**

Según la presente invención se facilita un método de detección de manipulación para imágenes digitales según la reivindicación 1 de las reivindicaciones acompañantes.

50 Preferiblemente, se aplica una transformada Fourier discreta a la imagen en base de bloque a bloque, y la filigrana es aplicada a cada uno de un número seleccionado de coeficientes DFT dentro de un bloque seleccionando la fase de dicho coeficiente DFT que sea igual a la fase de uno u otro de una pluralidad de valores de fase, de un conjunto de valores de fase cuantificados, que son más próximos a la fase real dependiendo del valor con que el bit filigranado ha de ser incrustado, y donde durante la recuperación de la filigrana, se toma de nuevo una transformada Fourier discreta
55 de cada bloque y la filigrana se recupera determinando a qué conjunto cuantificado de niveles los datos de fase del bit recuperados son más próximos.

60 Una medida de confianza para cada bit n de fase recuperada P_n puede ser definida como

$$C_n = 1 - (2 * |P_x - P_n| / |P_x - P_y|)$$

65 donde P_n es la fase recuperada para el bit n de la filigrana, $| \cdot |$ denota el módulo, y P_x , P_y son los niveles de fase de referencia más próximos, donde se eligió P_x como el nivel de fase más próximo.

Alternativamente, la filigrana digital se realiza en los bloques de la imagen de un tamaño predeterminado; donde un valor de amplitud se añade o resta de una amplitud relativa a cada uno de un número de píxeles seleccionados del bloque, dependiendo de si el valor con el que el bit filigranado ha de ser incrustado, y donde, durante la recuperación de la filigrana, se realiza una estimación del valor real, y donde cada valor de confianza se relaciona con la proximidad de la amplitud recuperada a uno o más de un conjunto cuantificado de niveles de amplitud de referencia. La medida de confianza C_n de cada bit n se puede definir entonces como

$$C_n = 1 - (2 * |A_x - A_n| / |A_x - A_y|)$$

donde A_n es la amplitud recuperada para el bit n de la filigrana, $||$ denota el módulo, y A_x , A_y son los niveles de amplitud de referencia más próximos, donde se eligió A_x como el más próximo.

La filigrana es preferiblemente un código binario (es decir el valor puede ser 0 o 1) o puede ser otros códigos, en que cada bit podría ser incrustado con tres, cuatro o más valores por ejemplo. Esta codificación puede ser útil en el dominio espacial, pero también puede ser usada en el dominio de transformada.

Breve descripción de los dibujos

Ahora se describirán realizaciones de la invención, a modo de ejemplo solamente, con referencia a los dibujos acompañantes, donde:

La figura 1 representa la DFT de un bloque que forma parte de una imagen.

La figura 2 representa niveles de cuantificación de fase para formar una filigrana.

La figura 3 representa un diagrama de fase en una etapa posterior de verificación de la filigrana.

La figura 4 representa valores de confianza a través de parte de una imagen.

La figura 5 representa variaciones del valor de confianza dependiendo de la posición de bit.

La figura 6 es un gráfico de valores de confianza y valores de varianza de magnitud DFT.

La figura 7 es un gráfico de valores de confianza para diferentes regímenes de compresión JPEG.

Y la figura 8 representa el efecto que tienen en la confianza cortar y pegar parte de una imagen.

Descripción detallada de realizaciones de la invención

Se describirán realizaciones de la invención que usan tipos de filigrana de imagen por modulación de fase. Sin embargo, se deberá apreciar que los conceptos de la presente invención se pueden aplicar igualmente con otros tipos de procesamiento de imagen, y en particular en el dominio espacial además del dominio de frecuencia o fase.

En un método en línea con el usado por Ruanaidh y colaboradores, una imagen se divide en bloques de tamaño deseado. Estos pueden ser, por ejemplo, de 16 x 16 píxeles. Se aplica una transformada Fourier discreta (DFT) al componente de luminancia de la imagen en base de bloque a bloque. La DFT genera un módulo y una fase. La figura 1 representa un bloque de 16x16 píxeles 1 que forma parte de una imagen 2. La filigrana es una cadena binaria de 1s y 0s que puede representar posiblemente un logo de compañía, un código de autenticación de usuario, información acerca de la fecha/hora/posición, etc. La filigrana se incrusta en el bloque 1 alterando la fase de coeficientes DFT seleccionados. Los coeficientes DFT seleccionados se representan de forma puramente esquemática como X_s en algunos de los coeficientes en bloque 1 de la figura 1. En algunas realizaciones, se usan 52 elementos (en la figura se representan menos para mayor claridad). El número 52 se elige para mínima visibilidad en la imagen, pero se pueden usar otros números a voluntad. La fase del coeficiente a usar se cuantifica a uno de un conjunto de valores como se representa en la figura 2. Aunque se puede usar cualquier número de niveles de fase P_0 a P_n , para un compromiso apropiado entre visibilidad y facilidad de recuperación, se ha hallado deseable usar ocho niveles de fase, P_0 a P_7 . La fase de cualquier coeficiente particular P_n serán modificada de modo que tome uno de los valores cuantificados $\{P_0... P_7\}$. Para tener un código binario, el esquema se elige de tal manera que si el bit de filigrana a incrustar es un 1, entonces se elige la fase más próxima del conjunto de fases pares $\{P_0, P_2, P_4, P_6\}$ para sustituir el valor P_n . Si el bit de filigrana a incrustar es un 0, entonces se elige el conjunto más próximo del conjunto de fases impares $\{P_1, P_3, P_5, P_7\}$ para sustituir el valor P_n .

En el extremo de recepción, con el fin de recuperar la filigrana, se toma la DFT de cada bloque de 16 x 16 y se examina la fase de los 52 bits filigranados. Si la fase recuperada es más próxima a uno del conjunto $\{P_0, P_2, P_4, P_6\}$, entonces se detecta un 1. Si la fase recuperada es más próxima a uno del conjunto $\{P_1, P_3, P_5, P_7\}$, entonces se detecta un 0.

Después de filigranar, la imagen puede experimentar una serie de operaciones legítimas tales como filtración no lineal, compresión JPEG, etc, que pueden alterar la fase de modo que la fase de la imagen recibida no sea más larga que lo determinado por el proceso de cuantificación de la figura 2. El receptor debe elegir entonces el nivel de cuantificación más próximo. La figura 3 representa un bit de la fase recibida P_0 . Obsérvese que la figura solamente
5 representa tres niveles de fase cuantificados para mayor claridad. Claramente, la fase original debe haber sido una de $P_0 \dots P_7$. Dado que P_0 es más próximo a P_1 , entonces el bit se considera que es un 0.

El método de detección esbozado con referencia a la figura 3 se basa en el supuesto de que ningún procesado intermedio legítimo no alterará la fase más allá del punto donde podría ser recuperada correctamente. Con referencia
10 a la figura, esto implica que si la fase P_n es alterada de forma significativa por procesado intermedio de modo que caiga por debajo de la línea de trazos 4 por ejemplo, entonces se detectará un 1 en lugar de un 0 porque la fase es más próxima a P_0 que P_1 .

Para mejorar la recuperación de la filigrana, la marca se puede repetir en cada uno de los bloques 16×16 de la imagen. Así, para una imagen QCIF (176×144 píxeles) habrá hasta 99 repeticiones de la filigrana (en la práctica no
15 todos los bloques son filigranados para reducir la visibilidad). Así, se puede tomar una media de todos los bloques que dé la filigrana recuperada. Sin embargo, la información dentro de cada bloque recibido puede ser usada con el fin de proporcionar más información acerca de qué ha sucedido en dicho bloque desde que se filigranó la imagen.

En realizaciones de la invención, una medida de confianza C_n para fase recuperada P_n se define como
20

$$C_n = 1 - (2 * |P_x - P_n| / |P_x - P_y|)$$

25 donde P_n es la fase recuperada para el bit n de la filigrana, $| \cdot |$ denota el módulo, y P_x, P_y son los niveles de fase de referencia más próximos, donde se eligió P_x como el más próximo. En el ejemplo representado en la figura 3, $P_x = P_1$, y $P_y = P_0$.

30 Así, si la fase P_n fuese igual a P_1 , se detectaría un 0 como el bit de filigrana con confianza 1. Si cayese a mitad de camino entre P_0 y P_1 (es decir, en la línea de trazos 4 de la figura 3), entonces no se sabría si deberá ser un 1 o un 0 de modo que la confianza de la decisión es 0.

35 Los procesos más legítimos tienden a operar en toda la imagen. Así, si se mide la medida de confianza para el bit n de la filigrana incrustada en el bloque de 16×16 K de la imagen, cabría esperar que fuese la misma que para el bit n de la filigrana realizada en cualquier otro bloque de 16×16 de la imagen. Si la medida de confianza C_n es la misma para el bit n en cada bloque, entonces es altamente improbable que la imagen haya sido manipulada. Por lo tanto, la posibilidad de que se haya producido manipulación puede ser detectada examinando la medida de confianza para el bit
40 n a través de la imagen completa, y en la figura 4 se representa la medida de confianza para algunos bits n . En la figura, se ha hallado que la confianza de recuperación del bit n de la filigrana es aproximadamente 0,8 para la mayor parte de los píxeles en la imagen (solamente se han representado unos pocos), pero una pequeña zona 5, que se representa sombreada, representa una confianza de 0,4. Por lo tanto, el usuario puede sospechar que en esta zona se realizó una operación que no se realizó en el resto de la imagen. Ejemplos de tal manipulación que impactarían en la confianza,
45 son cortar y pegar, donde la zona insertada puede tener o no su propia filigrana incrustada, filtración de dominio de frecuencia usando paquetes disponibles de manipulación de imágenes y otros tipos de procesado.

Consiguientemente, se sospecharía de esta imagen concreta y de su autenticidad.

50 Un método alternativo es calcular la confianza por bloque como una media a través de la filigrana completa y compararla con la medida de confianza media en cada uno de los otros bloques en toda la imagen. Una diferencia significativa en la medida de confianza para un bloque en comparación con el resto de la imagen podría indicar manipulación. Esta variación tiende a superar problemas que pueden tener lugar con un cambio localizado en la medida de confianza de un bit de la filigrana dentro de un bloque debido a ruido aleatorio u otros efectos aleatorios.

55 Se describe anteriormente cómo en algunas realizaciones no todos los bloques de la imagen pueden estar filigranados. Al determinar la confianza de la imagen, se esperaría que las zonas filigranadas tengan una medida de confianza más alta y, por lo tanto, un nivel de confianza más alto, que las que no han sido filigranadas. Así, en una modificación y para mejorar la seguridad, solamente se filigrana la zona seleccionada y la parte receptora tiene que conocer qué zonas lo están. Esto se puede hacer con un método clave. Dado que el receptor conoce entonces las zonas de la imagen que están filigranadas, esperaría ver medidas de confianza más altas en esa zona. Esto representa un nivel de seguridad adicional dado que un "hacker" puede conocer qué filigranas y niveles de confianza están siendo detectados, pero entonces será improbable que conozca en qué bloques concretos se deberá concentrar.

65 Es posible combinar los métodos de la presente invención con una medición de tasa de errores de bits (BER) de la filigrana recuperada por bloque, con respecto a la filigrana original (si se conoce), por ejemplo. Usando un BER al lado de la medida de confianza, se puede incrementar la seguridad y la confianza. Se puede usar un BER por sí solo, pero no detecta ciertos tipos de manipulación.

ES 2 332 033 T3

Cuando la invención se usa en el dominio espacial, entonces se pueden usar amplitudes en lugar de fases añadiendo o restando del valor de luminancia de los píxeles seleccionados un valor de amplitud (por ejemplo 2) dependiendo de si el bit ha de ser un 1 o 0 (es decir, añadiendo un valor si ha de ser 1, restando si ha de ser 0). En recuperación, se realiza una estimación del valor original y después se realiza una medición de confianza determinando qué cerca ha de estar el valor real de alguno de los dos valores esperados. Así, si el valor recuperado A_n está entre los valores esperados A_x y A_y , pero más próximo a A_x , la medida de confianza se define como sigue:

$$C_n = 1 - (2 * |A_x - A_n| / |A_x - A_y|)$$

Obsérvese que en lugar de un código binario, se puede incrustar un código diferente como una filigrana en algunas realizaciones, en los dominios tanto espacial como de transformada.

Anteriormente se ha descrito cómo un hacker puede saber, por ejemplo, que los bloques 16x16 están filigranados. Otra medida, que puede ser usada para mejorar la seguridad, es cambiar el origen de cada bloque. Con referencia de nuevo a la figura 1, el bloque 1 tiene su origen, es decir, el punto de inicio en el píxel C_0 . Entonces, el primer bloque sería normalmente el bloque superior izquierdo de la imagen, por ejemplo. En una técnica de cambio de origen, está decalado el origen desde el que posteriormente se mide cada bloque. Por ejemplo, el píxel O_1 puede ser usado como el origen. Esto decalará el bloque un píxel. El hacker tiene que conocer entonces no solamente el tamaño de los bloques, sino también el punto de origen de cada bloque y de nuevo esto mejora la seguridad. Claramente, la información relativa al decalado del origen tendrá que darse al receptor, pero esto lo podría hacer de nuevo un sistema de clave.

Las técnicas esbozadas anteriormente son muy eficientes en la mejora de la confianza en imágenes filigranadas. Sin embargo, a menudo las filigranas están distorsionadas y/o puede ser imposible recuperar cuando una imagen experimenta algún tipo de procesamiento legítimo tal compresión y descompresión JPEG.

La medida de confianza de la presente invención puede ser usada para detectar manipulación si se examina cada bloque en la imagen. Para hacerlo, la medida de confianza para el bit n en un bloque dado se compara con la medida para el bit n de la filigrana en todos los otros bloques de los valores. Los valores anómalos pueden ser evidencia de manipulación. Sin embargo, la medida de confianza propiamente dicha se puede someter a variación dentro de un bloque debido al impacto del procesamiento JPEG. Se logra procesamiento JPEG, como es conocido, por cuantificación de los coeficientes DCT (transformada de coseno discreto) de una imagen, que así impactan en la fase. Los bloques DCT en JPEG son de 8 x 8 píxeles y así hay cuatro bloques de 8 x 8 en un bloque de 16 x 16. La cuantificación JPEG no es constante en cada bloque de 8 x 8 píxeles, pero se define según una tabla de cuantificación. La cuantificación es cada vez más basta a medida que los coeficientes suben en frecuencia dado que el ojo es menos sensible a los componentes de alta frecuencia.

Un ejemplo del impacto del procesamiento JPEG en una filigrana de 52 bits se representa en la figura 5 donde el nivel de confianza como porcentaje se representa contra el número de bit de filigrana. Se ve en la figura que la medida de confianza varía dentro de la filigrana dependiendo de la posición del bit. Se indica una configuración cíclica que tiene picos y canales aproximadamente regulares cuya periodicidad depende de la relación entre la configuración de incrustamiento (y el tamaño de bloque usado para filigrana) y la cuantificación JPEG que se basa en bloques de 8 x 8 píxeles.

En modificaciones de la invención, un método simple de mejorar la confianza de recuperación de la filigrana sin destruir su fragilidad (que es esencial para la evidencia de manipulación) es desplazar el incrustamiento de la marca en cada bloque. Esto se puede hacer en una realización repitiendo la filigrana en cada bloque, pero girada un bit cada vez, como se representa en la tabla 1 siguiente.

TABLA 1

Bloque	Bit de inicio					Bit de fin
0	0	1	2	...	50	51
1	1	2	3	...	51	0
...						
99	47	48	49	...	45	46

Se apreciará que se puede usar otros muchos métodos de desplazamiento. La filigrana se puede girar más de un bit cada vez, puede ser desplazada entre bloques de manera pseudoaleatoria u otras muchas configuraciones y esquemas, como se apreciará.

ES 2 332 033 T3

El efecto de esta rotación o desplazamiento es que la confianza general de recuperación de la filigrana es ahora coherente en la media (es decir, tomando todos los bloques filigranados dentro de la imagen) para cada uno de los 52 bits. Además, se ha conservado la propiedad esencial de que se puede examinar la confianza para una posición de bit dada dentro de un bloque de 16 x 16 con referencia a la imagen completa, y así la filigrana se puede hacer más robusta (es decir, detectarse más fiablemente) sin afectar a sus propiedades de evidencia de manipulación.

Se deberá indicar que el método anterior no depende de ninguna periodicidad particular en la medida de confianza con respecto al número de bits de filigrana puesto que éste puede cambiar si los bits de filigrana se reordenan dentro del bloque de imagen en que están incrustados.

De nuevo, la modificación representada con referencia a la tabla 1 es igualmente aplicable en ambos sistemas de filigrana de dominio espacial y transformado. Es especialmente aplicable donde la imagen original y/o la filigrana original pueden no estar disponibles en el receptor cuando tiene lugar la detección de la filigrana.

La filigrana propiamente dicha puede tener un efecto visible en la imagen. Es importante elegir con cuidado las partes (es decir, los bloques) de la imagen que han de ser filigranados. Si la filigrana es demasiado visible, entonces es fácil que un hacker reproduzca la filigrana. Consiguientemente, para que sea exitoso, un esquema de filigrana y medida de confianza requiere bloques a filigranar que puedan tener una medida de confianza alta y también baja visibilidad.

Generalmente es prudente no filigranar zonas de una imagen que sean de baja textura.

Para esquemas de filigrana en el dominio de transformada de frecuencia en particular, pero también para uso en el dominio espacial, los inventores han hallado que se puede obtener información interesante mediante un estudio de la varianza de la magnitud de la transformada Fourier digital. La figura 6 representa tres gráficos. Un primer gráfico 6a es del nivel de confianza para algunos bloques en una imagen concreta. Las mediciones de confianza se representan como cuadrados y estos están unidos conjuntamente para formar un gráfico. Sobre éste se ha superpuesto otro gráfico 6b que representa la varianza de la magnitud de los coeficientes DFT de cada bloque. Un gráfico adicional 6c representa la magnitud media de los coeficientes DFT de los bloques que se seleccionaron para filigrana con respecto a la magnitud media de todos los coeficientes DFT del bloque.

Los niveles de varianza de la figura 6b se toman como porcentajes relevantes a la figura que tienen la varianza más alta, que se considera que es 100%.

Se aprecia que los niveles de confianza más altos se obtienen generalmente para las partes que tienen menor varianza (por ejemplo, los bloques 6d, 6e, 6f). Consiguientemente, para obtener los mejores resultados, es preferible elegir filigranar las partes de la imagen que tienen una varianza relativamente baja. En alguna realización estas pueden ser, por ejemplo, las partes de la imagen que tienen una varianza de menos de aproximadamente 50%. Si un bloque tiene una varianza de menos de 50%, entonces se considera que es un buen candidato para filigrana dado que este bloque tendrá entonces baja visibilidad y alta confianza.

Se ha hallado que configuraciones similares a la de la figura 6 se obtienen con la mayoría de las imágenes.

La tabla 2 siguiente muestra los efectos de filigranar tres imágenes diferentes, llamadas respectivamente "casa", "rosa" y "alubias", y de filigranar las partes de la imagen que tienen una varianza en la magnitud de DFT de menos de 50%. La confianza general varía de 75,5 a 89,78% y la visibilidad de las filigranas es buena (es decir, este significa que las filigranas no son especialmente visibles).

TABLA 2

Imagen de prueba	Número de bloques filigranados	BER general (%)	Confianza general (%)	PSNR medio (dB)	Visibilidad de filigrana
Casa	35	3,81	80,2	83,23	Buena
Rosa	60	6,99	75,5	78,5	Buena
Alubias	9	0,31	89,78	87,5	Buena

En cada una de las imágenes, un total de 64 bloques estaban disponibles para filigrana y solamente se eligieron algunos de estos para ser filigranados, dependiendo de si tenían la varianza correcta.

ES 2 332 033 T3

La tabla 3 siguiente indica los resultados de un segundo esquema para las tres mismas imágenes en que un bloque se filigranaba si la magnitud media de los 36 coeficientes DFT elegidos para filigrana era superior a 40% (es decir, 40% de la magnitud media total para el bloque DFT). Se ve que aunque aumenta la confianza general, la visibilidad de las filigranas no es tan buena como para los elegidos sólo cuando la varianza es inferior a 50%.

TABLA 3

Imagen de prueba	Número de bloques filigranados	BER general (%)	Confianza general (%)	PSNR media (dB)	Visibilidad de la filigrana
Casa	29	0,57	88,1	83,16	No tan buena como A
Rosa	33	3,68	80,1	75,0	Tan buena como A
Alubias	22	0,25	89,82	84,4	No tan buena como A

La tabla 4 siguiente indica un esquema en que se eligió un bloque a filigranar solamente si se cumplían ambas condiciones de las tablas 2 y 3, es decir, si la varianza de la magnitud de la DFT era inferior a 50% con respecto a la varianza máxima y la magnitud media de 36 coeficientes elegidos para filigrana era superior a 40% de la magnitud media total.

TABLA 4

Imagen de prueba	Número de bloques filigranados	BER general (%)	Confianza general (%)	PSNR media (dB)	Visibilidad de la filigrana
Casa	17	0,49	88,6	85,3	Tan buena como A
Rosa	30	3,85	81,1	79,5	A es ligeramente mejor
Alubias	9	0,31	89,8	87,6	Tan buena como A

Se aprecia que los niveles de confianza generales son altos y también que la visibilidad de las filigranas es buena.

Obsérvese que solamente un pequeño número de bloques cumplían los requisitos de esta tabla. Puede ser posible usar decalado de origen para cambiar el origen de modo que más bloques sean adecuados, y por ello maximizar el número de bloques que tienen las características preferidas para la filigrana.

Con referencia de nuevo a las imágenes de filigrana que después se someten a compresión JPEG, la figura 7 representa dos gráficos 7a y 7b de grados de compresión JPEG variables. 7a representa la confianza en los bloques que se sometieron a una compresión de 4:1, mientras que el bloque 7b representa los que se sometieron a una compresión de 11:1. Como se representa, los picos y canales en la medida de confianza están generalmente en línea, pero la mayor compresión tiende a reducir las amplitudes de los picos y canales. Así, las medidas de confianza pueden operar en una variación grande de imágenes y técnicas de compresión de imagen. Los valores de confianza cambian en formas predecibles para procesado legítimo.

ES 2 332 033 T3

La figura 8 representa los cambios en el nivel de confianza producidos cuando se manipulaba deliberadamente una imagen, en este caso cortando y pegando algunos bloques y partes de la imagen. El gráfico 8a indica los niveles de confianza por bloque, y el gráfico 8b muestra qué bloques fueron manipulados por corte y pegado. Se observa una correlación y el usuario puede determinar que la imagen puede haber sido manipulada y, por lo tanto, puede ser poco fiable como prueba.

10

15

20

25

30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Un método de detección de manipulación para imágenes digitales, incluyendo proporcionar una imagen con filigrana digital, y procesar digitalmente al menos algunas partes con filigrana de la imagen, **caracterizándose** el método porque el paso de procesamiento digital incluye determinar valores de confianza (5, 6a) para las al menos algunas partes con filigrana de la imagen, representando un valor de confianza la probabilidad de que una parte con filigrana ha sido manipulada y comparar los valores de confianza determinados a través de la imagen proporcionada para proporcionar una indicación acerca de la probabilidad de que la imagen proporcionada haya sido manipulada.

2. Un método según la reivindicación 1, donde el valor de confianza C_n de un bit n de la imagen proporcionada se relaciona con la proximidad de un valor recuperado del bit n , recuperado de la imagen proporcionada, a uno de los dos valores esperados.

3. Un método según la reivindicación 1 o 2, donde la filigrana digital se realiza en los bloques de la imagen de un tamaño predeterminado, donde se aplica una transformada Fourier discreta (DFT) a la imagen en base de bloque a bloque para generar una pluralidad de coeficientes DFT, y se aplica una filigrana a cada uno de un número seleccionado de coeficientes DFT dentro de un bloque seleccionando la fase de dicho coeficiente DFT (P_n) que sea igual a la fase de uno u otro de una pluralidad de valores de fase (P_1, P_2), de un conjunto de valores de fase cuantificados, que son más próximos a la fase real, dependiendo del valor con que el bit filigranado ha de ser incrustado, y donde durante la recuperación de la filigrana, se toma de nuevo una transformada Fourier discreta de cada bloque y la filigrana es recuperada determinando a qué conjunto cuantificado de niveles (F_1) están más próximos los datos de fase del bit recuperado, donde cada valor de confianza (6a) es relacionado con la proximidad de la fase recuperada a uno o más del conjunto cuantificado de niveles de fase.

4. Un método según la reivindicación 3, donde un valor de confianza para cada bit n de fase recuperada P_n se define como

$$C_n = 1 - (2 * |P_x - P_n| / |P_x - P_y|)$$

donde P_n es la fase recuperada para el bit n de la filigrana, $||$ denota el módulo, y P_x, P_y son los niveles de fase de referencia más próximos, donde P_x se eligió como el más próximo.

5. Un método según la reivindicación 1 o 2, donde la filigrana digital se realiza en los bloques de la imagen de un tamaño predeterminado; donde un valor de amplitud se añade o resta de una amplitud relativa a cada uno de un número de píxeles seleccionados del bloque, dependiendo de el valor con que el bit filigranado ha de ser incrustado, y donde durante la recuperación de la filigrana se realiza una estimación del valor real, y donde cada valor de confianza se relaciona con la proximidad de la amplitud recuperada a uno o más de un conjunto cuantificado de niveles de amplitud de referencia.

6. Un método según la reivindicación 5, donde un valor de confianza para cada bit es de amplitud recuperada A_n se define como:

$$C_n = 1 - (2 * |A_x - A_n| / |A_x - A_y|)$$

donde A_n es la amplitud recuperada para el bit n de la filigrana, $||$ denota módulos, y A_x, A_y son los niveles de amplitud de referencia más próximos, donde A_x se eligió como el más próximo.

7. Un método según cualquier reivindicación precedente, en que la imagen es filigranada en los bloques de tamaño predeterminado y donde se mide un valor de confianza C_n para el bit n en cada bloque y las medidas de confianza para el bit n a través de la imagen completa son comparadas posteriormente para determinar la probabilidad de manipulación.

8. Un método según cualquier reivindicación precedente, donde la imagen es filigranada en los bloques de tamaño predeterminado, y donde la confianza por bloque es medida como una media a través de la filigrana completa y se compara con el valor de confianza medio en cada uno de los otros bloques en toda la imagen, para determinar la probabilidad de manipulación.

9. Un método según cualquier reivindicación precedente, donde solamente una selección de bloques de tamaño predeterminado de la imagen se filigrana.

10. Un método según cualquier reivindicación precedente, donde la imagen es filigranada en los bloques de tamaño predeterminado y donde el origen de los bloques está decalado.

ES 2 332 033 T3

11. Un método según la reivindicación 10, donde se usa decalado de origen para maximizar el número de bloques adecuados para filigrana.

12. Un método según cualquier reivindicación precedente, donde la imagen es filigranada en los bloques de un tamaño predeterminado y donde el incrustamiento de la filigrana es desplazado de un bloque a otro.

13. Un método según la reivindicación 12, donde el desplazamiento incluye girar los bits de la filigrana de un bloque al siguiente según reglas predeterminadas, en particular donde el desplazamiento incluye un desplazamiento pseudoaleatorio de un bloque al siguiente.

14. Un método según cualquier reivindicación precedente, donde el proceso de filigrana incluye un paso de transformada Fourier discreta y donde las partes de la imagen elegida para filigrana son las que tienen una varianza de magnitud DFT seleccionada (6b).

15. Un método según la reivindicación 14, donde las zonas elegidas son las que tienen una varianza en la magnitud de los coeficientes de transformada Fourier discreta de menos de aproximadamente 50% con respecto a la varianza máxima de la magnitud DFT.

16. Un método según una de las reivindicaciones 14 o 15, donde las zonas elegidas son aquellas cuya magnitud media de los coeficientes DFT elegidos para filigrana es superior a aproximadamente 40% de la magnitud media total para el bloque completo (6c).

17. Un método según cualquier reivindicación precedente, donde la imagen es filigranada en los bloques y donde se usa una medición de tasa de errores de bits de la filigrana recuperada por bloque, con respecto a la filigrana original, en combinación con los valores de confianza para determinar la probabilidad de manipulación.

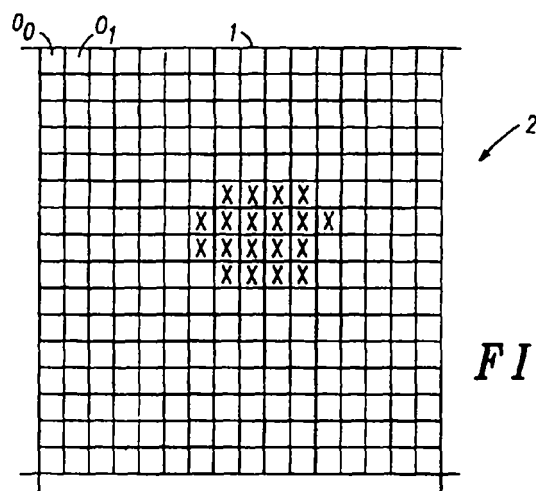


FIG. 1

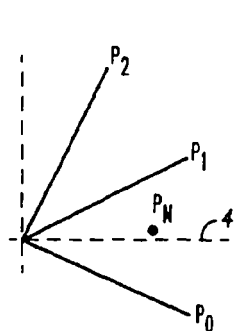


FIG. 3

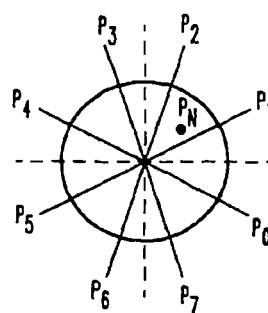


FIG. 2

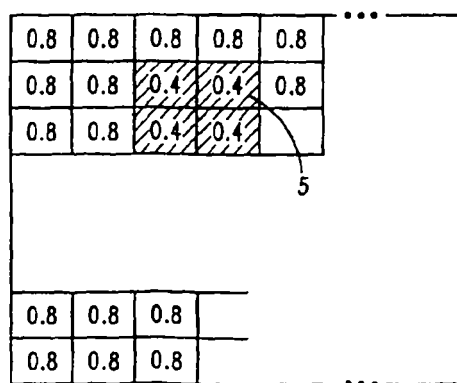


FIG. 4

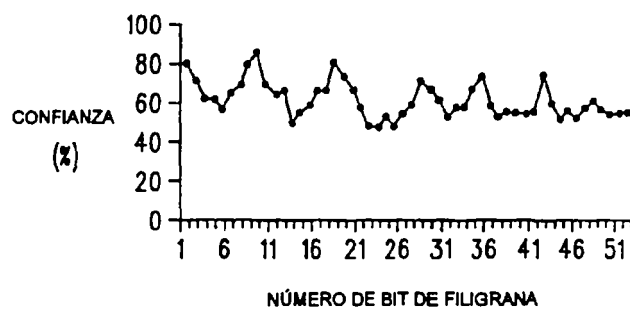


FIG. 5

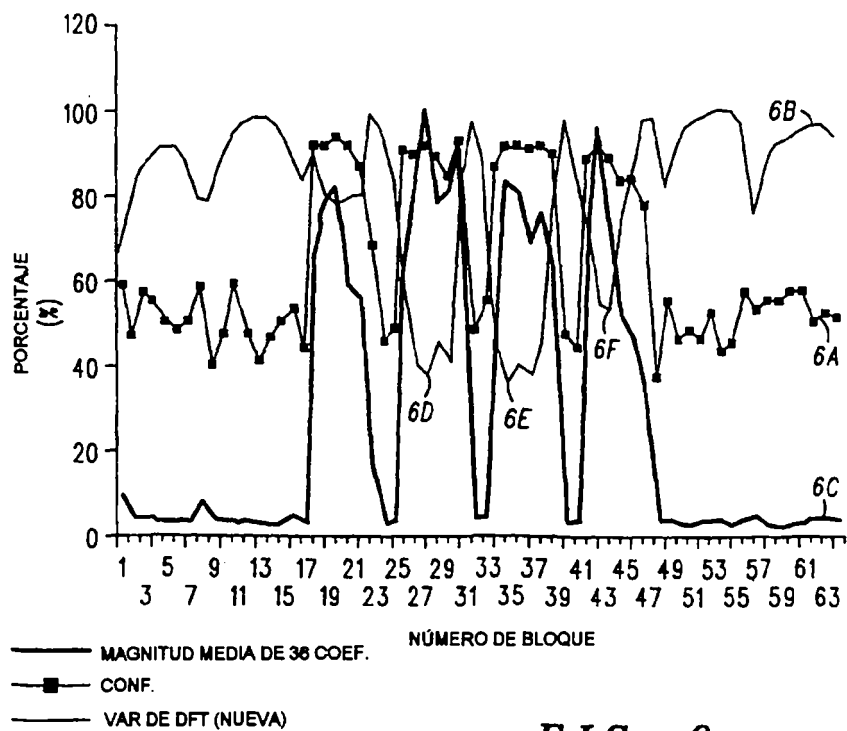


FIG. 6

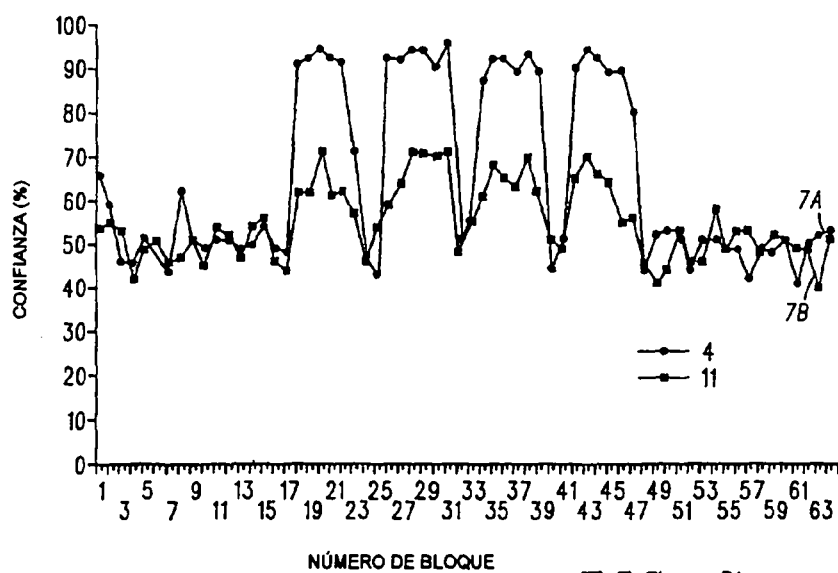


FIG. 7

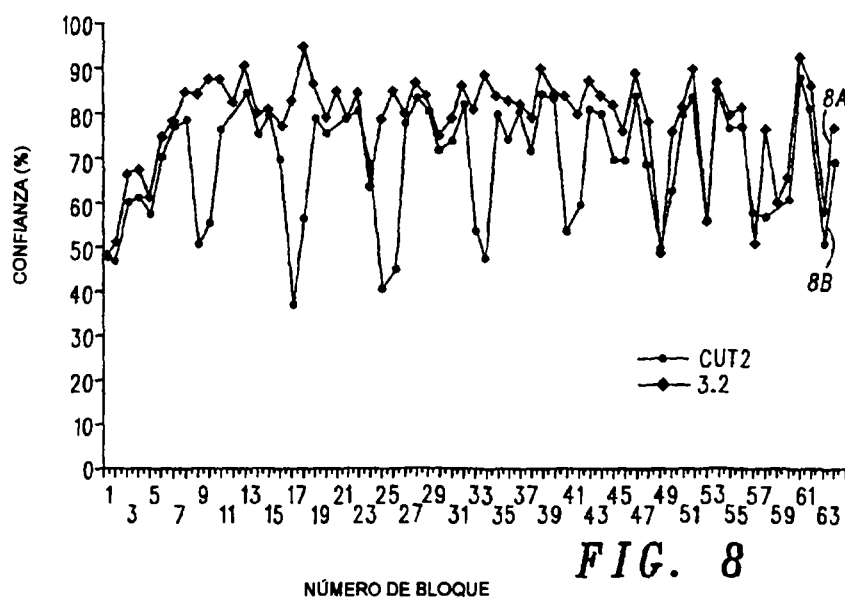


FIG. 8